The official voice of the Air Force Research Laboratory

news@afrl

Features

October 2003

Computer security research improves detection of insider attacks

by Fran Crum, Information Directorate

ROME, N.Y. — A paper presented at the MILCOM 2002 Military Communications Conference by Dr. Kevin Kwiat of the Air Force Research Laboratory's Information Directorate, has been featured in a Scientific American article. The article entitled "Keyboard Cops" resulted in developmental funding from the Defense Advanced Research Projects Agency (DARPA).

The paper described a joint effort between the Information Directorate and the State University of New York (SUNY) at Buffalo. The Associated Press released a story on the work that cited AFRL's involvement, and the story appeared in newspapers nation-wide and on numerous computer security-related websites.

The collaborative research began in 1998, when Dr. Shambhu Upadhyaya of SUNY Buffalo visited AFRL's Rome Research Site under the Summer Visiting Faculty Research Program with Dr. Kevin Kwiat as his mentor. Together they designed a user-level anomaly detection system for thwarting insider attackers. retired Air Force Lt. Gen. William Donahue, when he was director of Air Force Headquarters Communications and Information said, "We take our own networks down more with our own misdeeds."

The research was encouraging and reported in the MILCOM paper. Subsequently, Scientific American noted the paper and the work received exposure in the popular press. One outcome of this media visibility has been the recent funding by DARPA as a path-finding effort for a proposed program called "Self Regenerative Systems." Work is now underway to more fully develop the prototype and refine it with concepts from human and machine cognition.

Potential advantages of this research include future Air Force computer systems benefiting from the added protection afforded by the user-level anomaly detection system. More immediately, it contributes to AFRL's reputation as a "smart buyer" through the use of its basic research dollars to a stage of technology development where a Department of Defense customer is now providing continued funding. @